CLAIMS

What is claimed is:

1. A method for performing blind decryption of a message M, wherein said message is encrypted by a first node using an encryption function to form an encrypted message, the method comprising the steps of:

blinding said encrypted message with a blinding function z to form a blinded and encrypted message, wherein z has an inverse z^{-1};

in a first communicating step, communicating said blinded and encrypted message to a decryption agent;

decrypting said blinded and encrypted message by said decryption agent using a decryption function to form a blinded message, wherein said decryption function is the inverse of said encryption function;

in a second communicating step, communicating said blinded message to said first node; and

unblinding said blinded message using z^{-1}, to obtain said message M.

2. The method of claim 1 wherein said first node and said decryption agent are communicably coupled via a network, and at least one of said first and second communicating steps comprises the step of communicating the respective message over said network.

3. The method of claim 2 wherein said first and second communicating steps comprise communicating the respective messages over said network.

4. The method of claim 1 wherein said first communicating step comprises the step of communicating said blinded and encrypted

ATTORNEY DOCKET NO. P7898
WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

message from said first node to said decryption agent via an anonymizer node and said second communicating step comprises the step of communicating said blinded message from said decryption agent to said first node via said anonymizer node.

5. The method of claim 1 wherein said decryption function comprises an ephemeral decryption key.

6. The method of claim 5 further including the step of rendering said ephemeral decryption key unusable after a predetermined time.

7. The method of claim 1 further including the step of generating said message M at said first node.

8. The method of claim 1 wherein said encryption and decryption functions are, respectively, public and private keys of a public key pair.

9. The method of claim 8 wherein said public and private keys comprise a RSA public/private key pair of the form (e,n) and (d,n), respectively.

10. The method of claim 9 wherein said blinding function, z, is a blinding number R having an inverse R^{-1} that satisfies $R*R^{-1} = 1 \bmod n$ and wherein said blinding step includes the step of forming said blinded and encrypted message as the product ($R^e * M^e \bmod n$) where ($M^e \bmod n$) is said message M encrypted using said public encryption key.

ATTORNEY DOCKET NO. P7898
WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

11. The method of claim 10 wherein the decryption step includes raising the product $((R^e*M^e) \bmod n)$ to the power d mod n, forming $((R^e*M^e) \bmod n))^d \bmod n$ to form said blinded message R*M mod n.

12. The method of claim 11 wherein the unblinding step includes unblinding said blinded message R*M mod n using R^{-1} to obtain said message M.

13. The method of claim 10 further including the step of generating an integer random number and utilizing said random number as the blinding number R.

14. The method of claim 1 further comprising the steps of:

obtaining a public key associated with said decryption agent, wherein said public key is a Diffie-Hellman public key of the form $g^x \bmod p$;

selecting a blinding number, y, having an inverse blinding function y^{-1} that satisfies $y*y^{-1} = 1 \bmod p-1$;

raising said public key $g^x \bmod p$ to the power y to obtain $g^{xy} \bmod p$;

raising g to the power y to form $g^y \bmod p$;

encrypting said message M using $g^{xy} \bmod p$ to form said encrypted message of the form $\{M\}g^{xy} \bmod p$;

saving a copy of said encrypted message $\{M\}g^{xy} \bmod p$; and

saving a copy of $g^y \bmod p$ by said first node.

15. The method of claim 14 wherein said step of decrypting said blinded and encrypted message by said first node includes:

selecting a blinding number, w, having an inverse blinding number w^{-1} that satisfies $w*w^{-1} = 1 \bmod p-1$;

raising, by said first node, said public key $g^x \bmod p$ to the power w to obtain $g^{yw} \bmod p$;

ATTORNEY DOCKET NO. P7898
WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

forwarding g^{yw} mod p to said decryption agent;

receiving g^{xyw} mod p from said decryption agent; and

raising g^{xyw} mod p to said inverse blinding number, w^{-1}, to form g^{xy} mod p; and

decrypting said encrypted message $\{M\}g^{xy}$ mod p using g^{xy} mod p to obtain said message M.

16. The method of claim 14 wherein said blinding number, y, is a randomly selected integer.

17. The method of claim 15 wherein said blinding number, w, is a randomly selected integer.

18. The method of claim 1 further comprising the steps of:

selecting a blinding number y having an inverse blinding number y^{-1};

blinding said message M using said blinding number y to from a first blinded message;

forwarding said first blinded message to an encryption agent;

encrypting, by said encryption agent, said first blinded message to form a first blinded and encrypted message wherein said encryption is performed using said encryption function and wherein said encryption function and said corresponding decryption function are secret encryption and decryption keys, respectively;

forwarding said first blinded and encrypted message from said encryption agent to said first node; and

unblinding said first blinded and encrypted message using said inverse blinding number y^{-1} to form said encrypted message.

ATTORNEY DOCKET NO. P7898
WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

19. The method of claim 18 wherein step of blinding said message using said blinding number y to form said first blinded message includes the step of raising said message M to the power y mod p.

20. The method of claim 19 wherein said secret encryption key is a value x and wherein said secret decryption key is x^{-1} and wherein said step of encrypting said blinded message includes the step of raising said first blinded message M^y mod p to the power x mod p to form said first blinded and encrypted message

21. The method of claim 20 wherein said step of unblinding said first blinded and encrypted message includes the step of raising said first blinded and encrypted message M^{xy} mod p to the power y^{-1} mod p, to obtain said encrypted message M^x mod p.

22. The method of claim 21 wherein said step of decrypting said first blinded message by said decryption agent includes the step of raising said first blinded message to said secret decryption key x^{-1} to form a second blinded message M^z mod p.

23. A system for performing blind decryption of a message M comprising:

a first node and a decryption agent communicably coupled via a communications network;

said first node operative to:

encrypt said message using an encryption function to form an encrypted message;

blind said encrypted message with a blinding function z to form a blinded and encrypted message, wherein z has an inverse z^{-1};

ATTORNEY DOCKET NO. P7898
WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

communicate said blinded and encrypted message to a decryption agent;

decrypt said blinded and encrypted message by said decryption agent using a decryption function to form a blinded message, wherein said decryption function is the inverse of said encryption function;

communicate said blinded message to said first node; and

unblind said blinded message using z^{-1}, to obtain said message M.

24. A system for performing blind decryption of a message M comprising:

a first node and a decryption agent communicably coupled via a communications network;

means in said first node for:

blinding said encrypted message with a blinding function z to form a blinded and encrypted message, wherein z has an inverse z^{-1};

communicating said blinded and encrypted message to a decryption agent;

decrypting said blinded and encrypted message by said decryption agent using a decryption function to form a blinded message, wherein said decryption function is the inverse of said encryption function;

communicating said blinded message to said first node; and

unblinding said blinded message using z^{-1}, to obtain said message M.

25. A computer program product including a computer readable medium, said computer readable medium having a computer program

ATTORNEY DOCKET NO. P7898
WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

stored thereon for use in blinded ephemeral decryption, said computer program being executable on processors in a first node and a decryption agent respectively, said computer program product comprising:

program code for execution on said processor in said first node for blinding said encrypted message with a blinding function z to form a blinded and encrypted message, wherein z has an inverse z^{-1} and for communicating said blinded and encrypted message to a decryption agent;

program code for execution on said processor in said decryption agent for decrypting said blinded and encrypted message by said decryption agent using a decryption function to form a blinded message, wherein said decryption function is the inverse of said encryption function and for communicating said blinded message to said first node; and

program code for execution on said processor in said first node for unblinding said blinded message using z^{-1}, to obtain said message M.

ATTORNEY DOCKET NO. P7898
WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313